Claims

What is claimed is:

1. A cryptographically secure, computer hardware-implemented modular reduction method, comprising:

precomputing and storing in memory a constant U representing a bit-scaled reciprocal of a modulus M;

estimating an approximate quotient q for a number X to be reduced modulo M, wherein said estimating is executed upon X in a computation unit by a multiplication by said constant U and by bit shifts of X and a shift of said multiplication;

generating in a random number generator a random error value E and applying said error value to said approximate quotient to obtain a randomized quotient $q' = q - E$; and

calculating a remainder $R' = X - q'M$ in said computation unit, said remainder being larger than said modulus M but congruent to X modulo M.

2. The method of claim 1 wherein precomputing said constant U is performed according to the equation $U = \lfloor b^{2n+1}/M \rfloor$, where $b = 2^w$, with w being the word size of the computation unit in bits.

3. The method of claim 2 wherein estimating the approximate quotient q is performed by the computation unit according to the equation $q = \lfloor \left(\lfloor X/b^n \rfloor \cdot U \right) /b^{n+2} \rfloor$.

4. The method of claim 3 wherein a supplemental subtraction by one is included in the quotient estimation.

5. The method of claim 1 wherein the modular reduction of X is part of a computer hardware-implemented cryptography program.

6. The method of claim 1 wherein an alternate calculation pathway is provided wherein generating and applying an error value to the approximate quotient may be selectively omitted.

7. The method of claim 1 wherein the random number generator has a specified error limit of one-half word, whereby $0 \leq E < (2^{w/2} - 1)$.

8. Computational hardware for executing a cryptographically secure modular reduction method, the hardware comprising:

a computation unit adapted to perform word-wide multiply and accumulate steps on operands retrieved from a memory and carry terms from a set of registers;

a random number generator for generating a random error value E;

an operations sequencer comprising logic circuitry for controlling the computation unit and random number generator in accord with program instructions so as to carry out a modular reduction of a number X with respect to a modulus M that involves at least an estimation of an approximate quotient q from a pre-stored constant U representing a bit-scaled reciprocal of the modulus, a randomization of said the approximate quotient with said random error value E to obtain a randomized quotient $q' = q - E$, and a calculation of a remainder value $R' = X - q'M$.

9. The computation hardware of claim 8 further comprising operation parameter registers accessible by said operations sequencer, said registers containing any one or more of (a) pointers for locating operands within said memory, (b) information about lengths of operands, (c) carry injection control information for carry term registers, and (d) destination address information for intermediate results of operation steps.

10. The computation hardware of claim 8 wherein the pre-stored constant U in said memory is obtained from a precomputation according to the equation $U = \lfloor b^{2n+1}/M \rfloor$, where $b = 2^w$, with w being the word size of the computation unit in bits.

11. The computation hardware of claim 10 wherein the estimation of said approximate quotient q performed by said computation unit under control of said operations sequencer carrying out program instructions is done according to the equation $q = \lfloor \left(\lfloor X/b^n \rfloor \cdot U \right) /b^{n+2} \rfloor$.

12. The computation hardware of claim 11 wherein the quotient estimation performed by the computation unit includes a supplemental subtraction by one.

13. The computation hardware of claim 8 wherein the random number generator has a specified error limit of one-half word, whereby $0 \leq E < (2^{w/2} - 1)$.